CLAIMS

1. A method for authentication of communicating devices having a common secret, said method comprising the steps of:

receiving a hash by a receiving device from a sending device; and

comparing said hash received from said sending device with a hash of said receiving device, wherein both hashes are calculated by hash algorithms using identification data and said common secret.

2. The method of claim 1 wherein said identification data is generated by said sending device.

3. The method of claim 2 wherein said identification data is sent from said sending device to said receiving device.

4. The method of claim 1 wherein said hash algorithms are identical.

5. The method of claim 1 wherein said common secret comprises a PIN.

6. The method of claim 1 wherein said common secret comprises a password.

7. The method of claim 1 wherein said identification data is a random number.

8. The method of claim 7 wherein said random number is generated by an operating system of said sending device.

9. The method of claim 7 wherein said random number is generated by a separate software component which is part of said sending device.

10. The method of claim 1 wherein said comparing step is accomplished by said sending device.

11. The method of claim 1 wherein said comparing step is accomplished by said receiving device.

12. The method of claim 1 wherein said common secret, said hash algorithm and said comparing component of said sending device are stored in a smartcard and communication between smartcard and receiving device is established via a card reader.

13. The method of claim 12 wherein said smartcard and said card reader are part of a portable sending device.

14. The method of claim 1 wherein the data connection between the sending device and the receiving device is an insecure data connection.

15. The method of claim 1 wherein said sending device and said receiving device form a client-server architecture.

16. The method of claim 1 wherein said client is a portable device.

17. A client in a client-server architecture having an authentication system for executing the method of claim 1.

18. A server in a client-server architecture having an authentication system for executing the method of claim 1.

19. A sender device communicating with a receiver device, wherein one or both of said sender device and said receiver device comprise an authentication system for executing the method of claim 1.

20. A computer program product stored on a computer-readable medium containing software code for performing the method of claim 1 if the program product is executed on the computer.